

Functional safety and IEC 61508

A basic guide

November 2002

Copyright © IEC 2002. This material may be freely reproduced, except for advertising, endorsement or commercial purposes. The International Electrotechnical Commission (IEC) must be acknowledged as the source. All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced; nor is IEC in any way responsible for the other content or accuracy thereof.

Contents

	Page
1 Introduction	3
2 Functional safety	3
2.1 What is functional safety?	3
2.2 Safety functions and safety-related systems	3
2.3 Example of functional safety	4
2.4 Challenges in achieving functional safety.....	5
3 IEC 61508 – Functional safety of E/E/PE safety-related systems	5
3.1 Objectives	6
3.2 E/E/PE safety-related systems.....	6
3.3 Technical approach.....	7
3.4 Safety integrity levels	8
3.5 Example of functional safety revisited	8
3.6 Parts framework of IEC 61508	9
3.7 IEC 61508 as a basis for other standards	9
3.8 IEC 61508 as a stand-alone standard	11
3.9 Further information.....	11

1 Introduction

The purpose of this document is to introduce the concept of functional safety and give an overview of the international standard IEC 61508. You should read it if you are:

- wondering whether IEC 61508 applies to you,
- involved in the development of electronic or programmable systems which may have safety implications, or
- drafting any other standard where functional safety is a relevant factor.

Section 2 of this document gives an informal definition of functional safety, describes the relationship between safety functions, safety integrity and safety-related systems, gives an example of how functional safety requirements are derived, and lists some of the challenges in achieving functional safety in electronic or programmable systems. Section 3 gives details of IEC 61508, which provides an approach for achieving functional safety. The section describes the standard's objectives, technical approach and parts framework. It explains that IEC 61508 can be applied as is to a large range of industrial applications and yet also provides a basis for many other standards.

2 Functional safety

2.1 What is functional safety?

We begin with a definition of *safety*. This is freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment.

Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

For example, an overtemperature protection device, using a thermal sensor in the windings of an electric motor to de-energise the motor before they can overheat, is an instance of functional safety. But providing specialised insulation to withstand high temperatures is not an instance of functional safety (although it is still an instance of safety and could protect against exactly the same hazard).

2.2 Safety functions and safety-related systems

Generally, the significant hazards for equipment and any associated control system have to be identified by the specifier or developer via a hazard analysis. The analysis determines whether functional safety is necessary to ensure adequate protection against each significant hazard. If so, then it has to be taken into account in an appropriate manner in the design. Functional safety is just one method of dealing with hazards, and other means for their elimination or reduction, such as inherent safety through design, are of primary importance.

The term *safety-related* is used to describe systems that are required to perform a specific function or functions to ensure risks are kept at an accepted level. Such functions are, by definition, *safety functions*. Two types of requirements are necessary to achieve functional safety:

- *safety function requirements* (what the function does) and
- *safety integrity requirements* (the likelihood of a safety function being performed satisfactorily).

The safety function requirements are derived from the hazard analysis and the safety integrity requirements are derived from a risk assessment. The higher the level of safety integrity, the lower the likelihood of dangerous failure.

Any system, implemented in any technology, which carries out safety functions is a *safety-related system*. The safety-related system may be separate from any equipment control system or may be included within it. Higher levels of safety integrity necessitate greater rigour in the engineering of the safety-related system.

2.3 Example of functional safety

Consider a machine with a rotating blade that is protected by a hinged solid cover. The blade is accessed for routine cleaning by lifting the cover. The cover is interlocked so that whenever it is lifted an electrical circuit de-energises the motor and applies a brake. In this way the blade is stopped before it could injure the operator.

In order to ensure that safety is achieved, both hazard analysis and risk assessment are necessary.

- 1) The *hazard analysis* identifies the hazards associated with cleaning the blade. For this machine it might show that it should not be possible to lift the hinged cover more than 5 mm without the brake activating and stopping the blade. Further analysis could reveal that the time for the blade to stop must be one second or less. Together, these describe the *safety function*.
- 2) The *risk assessment* determines the performance requirements of the safety function. The aim is to ensure that the *safety integrity* of the safety function is sufficient to ensure that no one is exposed to an unacceptable risk associated with this hazardous event.

The safety integrity of the safety function will depend on all the equipment that is necessary for the safety function to be carried out correctly, i.e. the interlock, the associated electrical circuit and the motor and braking system.

The harm resulting from a failure of the safety function could be amputation of the operator's hand or could be just a bruise. The risk also depends on how frequently the cover has to be lifted, which might be many times during daily operation or might be less than once a month. The level of safety integrity required increases with the severity of injury and the frequency of exposure to the hazard.

To summarise, the hazard analysis identifies what has to be done to avoid the hazardous event, or events, associated with the blade. The risk assessment gives the safety integrity required of the interlocking system for the risk to be acceptable. These two elements, “what safety function has to be performed” – the *safety function requirements* – and “what degree of certainty is necessary that the safety function will be carried out” – the *safety integrity requirements* – are the foundations of functional safety.

2.4 Challenges in achieving functional safety

Safety functions are increasingly being carried out by electrical, electronic or programmable electronic systems. These systems are usually complex, making it impossible in practice to fully determine every failure mode or to test all possible behaviour. It is difficult to predict the safety performance, although testing is still essential.

The challenge is to design the system in such a way as to prevent dangerous failures or to control them when they arise. Dangerous failures may arise from:

- incorrect specifications of the system, hardware or software;
- omissions in the safety requirements specification (e.g. failure to develop all relevant safety functions during different modes of operation);
- random hardware failure mechanisms;
- systematic hardware failure mechanisms;
- software errors;
- common cause failures;
- human error;
- environmental influences (e.g. electromagnetic, temperature, mechanical phenomena);
- supply system voltage disturbances (e.g. loss of supply, reduced voltages, re-connection of supply).

IEC 61508 contains requirements to minimise these failures and is described in the next section.

3 IEC 61508 – Functional safety of E/E/PE safety-related systems

3.1 Objectives

The international standard IEC 61508, *Functional safety of electrical/electronic/ programmable electronic (E/E/PE) safety-related systems* aims to:

- release the potential of E/E/PE technology to improve both safety and economic performance;
- enable technological developments to take place within an overall safety framework;
- provide a technically sound, system based approach, with sufficient flexibility for the future;
- provide a risk-based approach for determining the required performance of safety-related systems;
- provide a generically-based standard that can be used directly by industry but can also help with developing sector standards (e.g. machinery, process chemical plants, medical or rail) or product standards (e.g. power drive systems);
- provide a means for users and regulators to gain confidence when using computer-based technology;
- provide requirements based on common underlying principles to facilitate:
 - improved efficiencies in the supply chain for suppliers of subsystems and components to various sectors,
 - improvements in communication and requirements (i.e. to increase clarity of what needs to be specified),
 - the development of techniques and measures that could be used across all sectors, increasing available resources,
 - the development of conformity assessment services if required.

IEC 61508 does not cover the precautions that may be necessary to prevent unauthorized persons damaging, and/or otherwise adversely affecting, the functional safety achieved by E/E/PE safety-related systems.

3.2 E/E/PE safety-related systems

IEC 61508 is concerned with functional safety, achieved by safety-related systems that are primarily implemented in electrical and/or electronic and/or programmable electronic (E/E/PE) technologies, i.e. E/E/PE safety related systems. The standard is generic in that it applies to these systems irrespective of their application.

Some requirements of the standard relate to development activities where the implementation technology may not yet have been fully decided. This includes development of the overall

safety requirements (concept, scope definition, hazard analysis and risk assessment). If there is a possibility that E/E/PE technologies might be used, the standard should be applied so that the functional safety requirements for any E/E/PE safety-related systems are determined in a methodical, risk-based manner.

Other requirements of the standard are not solely specific to E/E/PE technology, including documentation, management of functional safety, functional safety assessment and competence. All requirements that are not technology-specific might usefully be applied to other safety-related systems although these systems are not within the scope of the standard.

The following are examples of E/E/PE safety-related systems:

- emergency shut-down system in a hazardous chemical process plant;
- crane safe load indicator;
- railway signalling system;
- guard interlocking and emergency stopping systems for machinery;
- variable speed motor drive used to restrict speed as a means of protection;
- system for interlocking and controlling the exposure dose of a medical radiotherapy machine;
- dynamic positioning (control of a ship's movement when in proximity to an offshore installation);
- fly-by-wire operation of aircraft flight control surfaces;
- automobile indicator lights, anti-lock braking and engine-management systems;
- remote monitoring, operation or programming of a network-enabled process plant;
- an information-based decision support tool where erroneous results affect safety.

An E/E/PE safety-related system covers all parts of the system that are necessary to carry out the safety function (i.e. from sensor, through control logic and communication systems, to final actuator, including any critical actions of a human operator).

Both safety and E/E/PE safety-related systems are defined in terms of freedom from unacceptable risk of physical injury and of damage to the health of people. The harm can arise to people directly, or indirectly as a result of damage to property or the environment. But some systems will be designed primarily to protect against failures with serious economic implications. IEC 61508 can be used to develop any E/E/PE system that has critical functions, such as the protection of equipment or products.

3.3 *Technical approach*

IEC 61508:

- uses a risk based approach to determine the safety integrity requirements of E/E/PE safety-related systems, and includes a number of examples of how this can be done.
- uses an overall safety lifecycle model as the technical framework for the activities necessary for ensuring functional safety is achieved by the E/E/PE safety-related systems.
- covers all safety lifecycle activities from initial concept, through hazard analysis and risk assessment, development of the safety requirements, specification, design and implementation, operation and maintenance, and modification, to final decommissioning and/or disposal.
- encompasses system aspects (comprising all the subsystems carrying out the safety functions, including hardware and software) and failure mechanisms (random hardware and systematic).
- contains both requirements for preventing failures (avoiding the introduction of faults) and requirements for controlling failures (ensuring safety even when faults are present).
- specifies the techniques and measures that are necessary to achieve the required safety integrity.

3.4 *Safety integrity levels*

IEC 61508 specifies 4 levels of safety performance for a safety function. These are called safety integrity levels. Safety integrity level 1 (SIL1) is the lowest level of safety integrity and safety integrity level 4 (SIL4) is the highest level. The standard details the requirements necessary to achieve each safety integrity level. These requirements are more rigorous at higher levels of safety integrity in order to achieve the required lower likelihood of dangerous failure.

An E/E/PE safety-related system will usually implement more than one safety function. If the safety integrity requirements for these safety functions differ, unless there is sufficient independence of implementation between them, the requirements applicable to the highest relevant safety integrity level shall apply to the entire E/E/PE safety-related system.

If a single E/E/PE system is capable of providing all the required safety functions, and the required safety integrity is less than that specified for SIL1, then IEC 61508 does not apply.

3.5 *Example of functional safety revisited*

The safety function requirements and the safety integrity requirements constitute the functional safety requirements specification. These requirements must be fully determined before designing the E/E/PE safety-related system.

In the example described in section 2, the functional safety requirements for the specific hazardous event could be stated as follows.

When the hinged cover is lifted by 5 mm or more, the motor shall be de-energised and the brake activated so that the blade is stopped within 1 second. The safety integrity level of this safety function shall be SIL2.

The E/E/PE safety-related system includes the guard interlock switch, the electrical circuit, contactors, the motor and the brake.

3.6 Parts framework of IEC 61508

IEC 61508, titled *Functional safety of electrical/electronic/programmable electronic safety-related systems*, consists of 7 parts:

- IEC 61508-1, General requirements;
- IEC 61508-2, Requirements for electrical/electronic/programmable electronic safety-related systems;
- IEC 61508-3, Software requirements;
- IEC 61508-4, Definitions and abbreviations;
- IEC 61508-5, Examples of methods for the determination of safety integrity levels;
- IEC 61508-6, Guidelines on the application of IEC 61508-2 and IEC 61508-3;
- IEC 61508-7, Overview of measures and techniques.

A requirements map is shown in figure 1.

3.7 IEC 61508 as a basis for other standards

Standards writers need to address functional safety in their safety standard if the hazard analysis carried out by a Technical Committee identifies that this is necessary to adequately protect against a significant hazard or hazardous event.

Parts 1, 2, 3 and 4 of IEC 61508 are *IEC basic safety publications*. One of the responsibilities of IEC Technical Committees is, wherever practicable, to make use of these parts of IEC 61508 in the preparation of their own sector or product standards that have E/E/PE safety-related systems within their scope. For more details see *IEC Guide 104, The preparation of safety publications and the use of basic safety publications and group safety publications* and *ISO/IEC Guide 51, Safety aspects – Guidelines for their inclusion in standards*.

IEC 61508 is the basis for a published nuclear sector standard. It is also currently being used as a basis for developing other sector standards (e.g. machinery, process) and product standards (e.g. power drive systems). It is therefore influencing the development of E/E/PE safety-related systems and products across all sectors. Sector specific standards are facilitated by a distinction between requirements concerning the application of the E/E/PE safety-related system (which are often sector specific), and detailed design requirements

(which are mostly sector independent). The sector independent requirements lie between the safety requirements allocation and overall installation and commissioning phases of the overall safety lifecycle. These will usually be referenced rather than repeated in the application sector or product standards. Consequently most users will need IEC 61508 also.

The basic safety publication status of IEC 61508 described above does not apply in the context of low complexity E/E/PE safety-related systems. These are E/E/PE safety-related systems in which the failure modes of each individual component are well defined and the behaviour of the system under fault conditions can be completely determined. An example is a system comprising one or more limit switches, operating one or more contactors to de-energize an electric motor, possibly via interposing electromechanical relays.

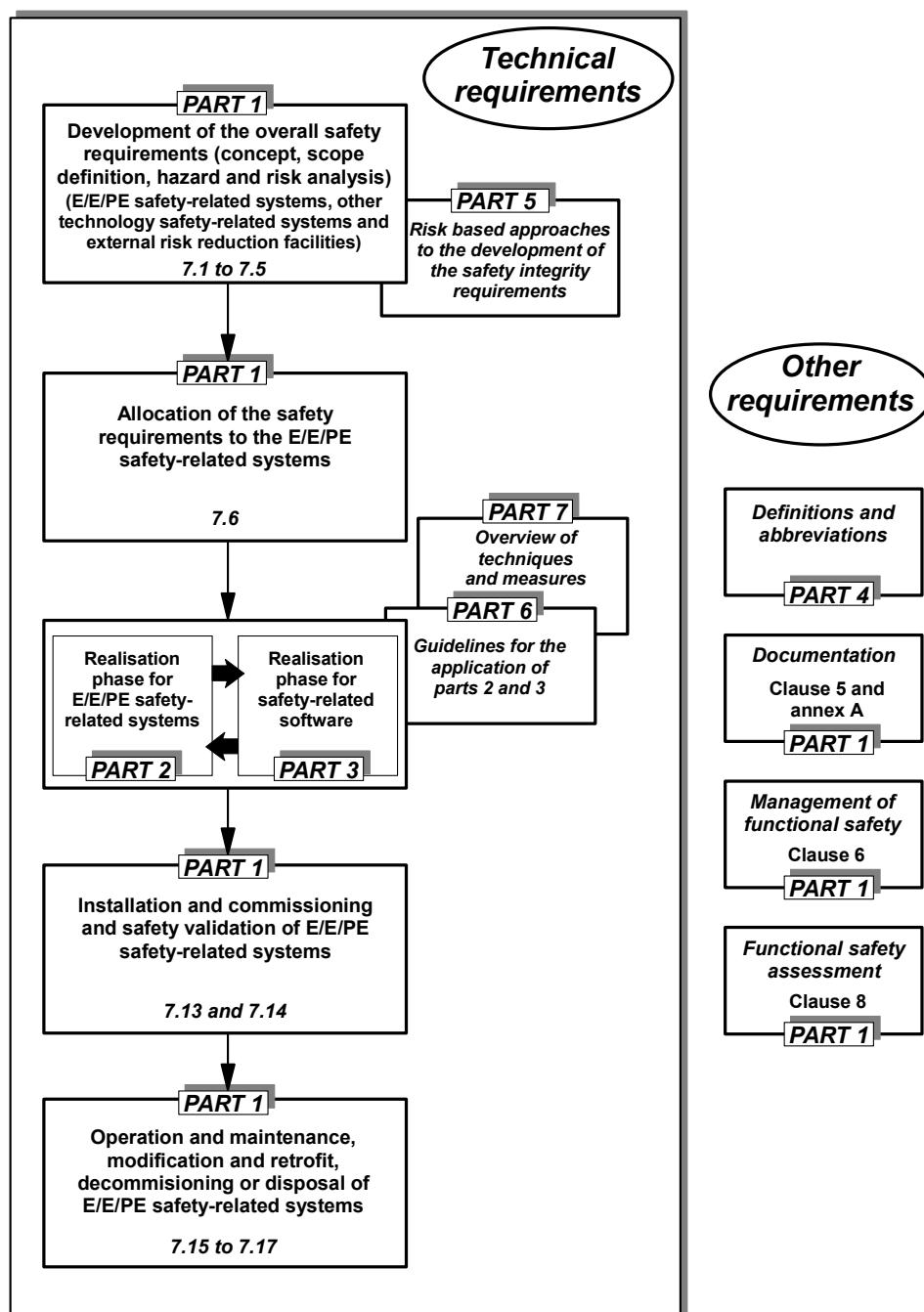


Figure 1: Requirements map for parts 1 to 7 of IEC 61508

3.8 IEC 61508 as a stand-alone standard

All parts of IEC 61508 can be used directly by industry as “stand-alone” publications. This includes use of the standard:

- as a set of general requirements for E/E/PE safety-related systems where no application sector or product standards exist or where they are not appropriate;
- by suppliers of E/E/PE components and subsystems for use in all sectors (e.g. hardware and software of sensors, smart actuators, programmable controllers);
- by system builders to meet user specifications for E/E/PE safety-related systems;
- by users to specify requirements in terms of the safety functions to be performed together with the performance requirements of those safety functions;
- to facilitate the maintenance of the "as designed" safety integrity of E/E/PE safety-related systems;
- to provide the technical framework for conformity assessment and certification services;
- as a basis for carrying out assessments of safety lifecycle activities.

3.9 Further information

You can find further information on IEC 61508 and functional safety, including details on how to obtain the standard, in the Functional Safety Zone of the IEC web site (<http://www.iec.ch/functionalsafety>).

If you have a copy of the standard but are not familiar with its contents, you may find it helpful to read the following sections first:

- Annex A of IEC 61508-5, which introduces risk concepts and safety integrity.
- Figure 2 and table 1 of IEC 61508-1, which illustrate the overall safety lifecycle and list the objectives of each lifecycle phase. The lifecycle and phase objectives provide a key to understanding the requirements of clause 7 of IEC 61508-1.
- Clauses 6 and 8 of IEC 61508-1, which contain requirements relating to management of functional safety and functional safety assessment.
- Annex A of IEC 61508-6, which gives an eight-page overview of the requirements in IEC 61508-2 and IEC 61508-3.
- Figure 2 and table 1 of IEC 61508-2 and figure 3 and table 1 of IEC 61508-3, which provide a key to understanding the requirements of clause 7 of IEC 61508-2 and IEC 61508-3 respectively.

Any particular requirement of IEC 61508 should be considered in the context of its lifecycle phase (where applicable) and the stated objectives for the requirements of that phase, clause or subclause. The objectives are always stated immediately before the requirements.